



# National Infrastructure Protection Center NIPC Daily Open Source Report for 30 January 2003

Current Nationwide  
Threat Level is



[For info click here](#)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- The Palm Beach Post reports natural gas leaking from a corroded underground 3-inch pipe into surrounding storm sewer and utility pipes, forced the evacuation of some residents Monday – – the second such leak in as many weeks in a Florida Public Utilities line. (See item [2](#))
- The Financial Times reports Japan has admitted that 206kg of its plutonium – enough to make about 25 nuclear bombs – is unaccounted for. (See item [4](#))
- CNN reports a massive explosion blew apart a pharmaceutical supply plant Wednesday, injuring more than two dozen people — at least eight of them critically — and sending clouds of black smoke billowing into the sky. (See item [8](#))
- The Washington Post reports President Bush announced plans Tuesday night for a new center to integrate intelligence on terrorism collected at home and abroad, saying it was necessary to create the most comprehensive picture of possible threats to the United States and its citizens. (See item [31](#))
- Government Computer News reports the failure of many organizations to apply a patch that had been available since the summer contributed to the spread of the worm known as "SQL Slammer" which infected an estimated 250,000 servers over the weekend. (See item [40](#))
- Editors note: The NIPC Daily Report is now available on the NIPC homepage in both PDF and Word format. It can be found at: <http://www.nipc.gov/dailyreports/dailyindex.htm>.

### **NIPC Update *Fast Jump***

**Production Industries:** [Energy](#); [Chemical](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [General](#); [NIPC Web Information](#)

## **Energy Sector**

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *January 29, Agence France Presse* — **Ukraine, source of radioactive worry for U.S. Former Soviet Ukraine has all the ingredients for sending the West into nuclear shock: mounds of uranium, impoverished but top-notch scientists, and worse still, an open interest in the cash of countries like Iraq.** One nuclear institute in the northeastern city of Kharkiv, where Iraq opened an official mission in 2000, has particularly furrowed Washington's brow. It's Physics and Technology Institute (IPTK) reportedly stores 75 kilograms (165 pounds) of enriched uranium, enough to build three nuclear bombs, according to experts. **The United States is eager to buy that uranium off IPTK to make sure it does not end up in the wrong hands. "Americans have asked us to sell them this uranium. But we refused. We don't intend to sell it to anyone,"** IPTK's director Volodymyr Lapshin told Agence France Presse, at the same time refusing to confirm the exact amount of uranium stored in his institute. **Kharkiv has been visited by three Iraqi delegations since the Baghdad mission opened its doors.** One of those stopped over at the immense IPTK center, which in Soviet times boasted up to 50,000 staff. Today the overwhelming majority of those researchers struggle to survive on a monthly salary of about 150 dollars (140 euros), forcing many to seek funds elsewhere. But other dangers lurk in Ukraine, site to the world's worst peace-time nuclear disaster in 1986. **According to Sergy Kondratov, a physicist affiliated with Ukraine's Academy of Sciences, "the trafficking in radioactive metals from Chernobyl's central reactor, which has been closed for two years now, is in fact a worse problem than the well-guarded Kharkiv uranium."** The Chernobyl nuclear power plant seared itself into the world's consciousness on April 26, 1986 when a reactor blew up, spewing out a radioactive cloud and contaminating much of Europe.

Source: [http://www.dailytimes.com.pk/default.asp?page=story\\_29-1-2003\\_pg4\\_9](http://www.dailytimes.com.pk/default.asp?page=story_29-1-2003_pg4_9)

2. *January 29, Palm Beach Post* — **Buried pipe leaks gas into sewer, utility lines. Natural gas leaking from an underground pipe forced the evacuation of some residents Monday – – the second such leak in as many weeks in a Florida Public Utilities line.** The gas seeped from a corroded 3-inch pipe into surrounding storm sewer and utility pipes, from there wafting above ground through manhole covers and drains around Spruce Avenue and 15th Street. Residents reported the rotten-egg smell of gas about 2:30 p.m. and police evacuated the area shortly thereafter, officials said. When West Palm Beach firefighters threaded monitors into the pipes, some showed dangerous levels of gas. "Any spark, any flame and it could have gone 'boom,' " said Capt. Matt Young, head of the hazardous materials team. A Florida Public Utilities supervisor on scene declined to comment about the exact cause of the leak, saying said the company would issue a written statement today. **Two weeks ago, another leak forced evacuations and put a neighborhood on alert. On Jan. 10, a rupture in a natural gas line in Lake Worth sent a 30-foot plume of vapor into the air just yards away from Tri-Rail tracks, Interstate 95 and the city power plant. The gas forced hundreds of students to evacuate classrooms at Lake Worth High School and sent 14 students and staff members sickened by the smell to the hospital. The leading cause of pipeline leaks is from an outside source, such as construction crews or traffic accidents. The second leading cause is corrosion – believed to be the cause of Monday's West Palm Beach leak.**

Source: [http://www.energycentral.com/sections/gasnews/gn\\_article.cfm?id=3602020](http://www.energycentral.com/sections/gasnews/gn_article.cfm?id=3602020)

3.

*January 28, PR Newswire* — **Energy commission predicts promising electricity supply and demand for next five years.** The California Energy Commission predicts that electricity demand and supply for the State looks promising this summer, and supplies should continue to remain positive through the year 2005. According to testimony the Energy Commission presented Tuesday before the State Senate Energy Committee, California should have a nine percent operating reserve during the critical summer months of July, August, and September, even without counting spot market imports that might be needed under extremely hot weather conditions. When the expected spot market purchases from outside the State are included in the forecast, operating reserves increase to 15 percent during the most critical months. Analysis by Energy Commission staff finds that California's power situation has improved since the Electricity Crisis of 2000. **First, 18 new power plants have been licensed and constructed, adding over 4,980 megawatts to the grid. By August 2003, seven additional power plants generating 3,106 more megawatts will come online. Also, 25 renewable energy power plants -- adding nearly 110 megawatts -- have been funded through the Energy Commission's New Renewable Account, with an additional 12 megawatts coming on line before August, 2003. Second, as a result of emergency energy legislation, energy efficiency projects are now in place to save electricity at critical peak-load times. These yield over 1,100 megawatts of savings from programs such as installing real time meters, implementing energy efficiency measures in State buildings, retrofitting equipment at waste water treatment facilities and installing LED traffic lights. Third, California is not the only state constructing new power plants to meet growing electricity demand throughout the West.** Natural gas prices have declined from their high levels in 2000 through 2001 and electricity contracts signed in 2001 by the California Department of Water Resources have ensured that there will be sufficient capacity to meet load.

Source: [http://hsweb01.screamingmedia.com/PMA/pma\\_newsarticle1\\_national.htm?SMDOCID=comtex\\_2003\\_01\\_28\\_pr\\_0000-3761-ca-ca-energy-predicta](http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=comtex_2003_01_28_pr_0000-3761-ca-ca-energy-predicta)>

4. *January 28, Financial Times* — **Japan 'loses' 206kg of plutonium.** Japan on Tuesday admitted that 206kg of its plutonium – enough to make about 25 nuclear bombs – is unaccounted for. Government scientists said that 6,890kg of plutonium had been extracted since 1977 from spent nuclear fuel at a processing plant about 120km north east of Tokyo. But that is 3 per cent short of the amount the plant was estimated to have produced. About 5kg to 8kg of plutonium are needed to make a 20-kiloton atomic bomb similar to the one that destroyed Nagasaki in 1945. Experts said the missing amount was surprisingly large. Japan's admission comes at a time of acute sensitivity because of the threat of nuclear proliferation in north-east Asia following North Korea's revival of its mothballed nuclear programme. However, there is no evidence that North Korea was linked to the missing plutonium even though it is known to smuggle goods in and out of Japan. **"This is an unusually large amount of plutonium to be unaccounted for, which makes me uncomfortable, although I think it's highly unlikely that it was stolen,"** said Tatsujiro Suzuki, senior research scientist at the Central Research Institute of Electric Power Industry. The IAEA, the United Nations nuclear watchdog, has urged Japan to strengthen its procedures for measuring nuclear material since it first noted discrepancies in 1998.

Source: <http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory42491288304/a>>

5. *January 28, Reuters* — **FERC urged to give states more say over grid rules.** The Federal

Energy Regulatory Commission (FERC) must give state utility regulators a bigger role in planning transmission projects to win support for FERC's planned rules for U.S. electricity markets, major U.S. utilities said on Tuesday. FERC, which proposed a set of market rules last summer, faces bitter opposition from Southern and Western states, which fear the authority of their state regulators will be usurped. **The proposed rules would combine U.S. regional transmission networks, launch real-time trading and create market monitors to detect unfair trades, beginning in 2004 in some regions. The plan aims to avoid a repetition of the California energy crisis of 2000-01, when wholesale power prices rocketed amid blackouts and billions of dollars in state economic losses. However, the plan has drawn fire from Southern and Western states, which already enjoy cheap electricity and fear the new market rules would mean higher costs for consumers.** The Edison Electric Institute, an industry lobbying group representing the largest U.S. utilities, said the FERC must give states a greater advisory role to determine which transmission projects get built, the Edison trade group told FERC in a filing. The proposed rules would give that authority to regional planning groups. Source: [http://www.energycentral.com/sections/newsroom/nr\\_article.cf m?id=3601922](http://www.energycentral.com/sections/newsroom/nr_article.cf m?id=3601922)

6. *January 28, News Sentinel* — **TVA plans to add 18 windmills on Buffalo Mountain. Eighteen huge new windmills are expected to be whirling atop Buffalo Mountain by year's end, TVA will announce today. TVA has signed a 20-year power purchase agreement with Invenergy LLC, a Chicago-based energy development company, to build and operate the wind turbines.** The turbines, each about 300 feet tall, will be erected on either side of the three windmills that have been spinning at the crest of 3,300-foot-tall Buffalo Mountain for three years. **The additions will also increase by 10-fold the amount of power generated by TVA's latest venture into renewable energy sources. The new turbines will provide enough wind generation to power 4,500 homes, TVA officials said.** Anderson County Executive Rex Lynch said he welcomes the new windmills. "We've proven in this area that wind is an alternative energy source," he said. Invenergy will develop, engineer, finance, build, own and operate the 18 new wind turbines. Each can produce more than twice as much electricity as the three windmills now on the mountaintop. Work on the new turbines will begin in the spring, and they should be in operation by November, said Enio Ricci, vice president of Invenergy. Each new windmill will cost between \$1 million and \$1.5 million, he said. Source: [http://www.energycentral.com/sections/newsroom/nr\\_article.cf m?id=3601948](http://www.energycentral.com/sections/newsroom/nr_article.cf m?id=3601948)

7. *January 28, Reuters* — **Cold drives U.S. East Coast power demand to record.** Two weeks of biting cold pushed winter electricity demand in the U.S. Mid-Atlantic states to record highs, the region's grid operator said Tuesday. **Grid operator PJM Interconnection said power demand from utilities in the region peaked on Jan 23 at 55,031 megawatts, when the average daytime high in the region was a bone-chilling 17 degrees Fahrenheit (minus 8 C), shattering the previous record of 50,864 MW hit just two days earlier.** Until this past week, the winter record for power demand in PJM was 50,129 MW, set Jan 27, 2000. One megawatt of electricity is enough to power about 1,000 average homes. With forecasters predicting an end Wednesday to the current cold snap, this latest record is likely to stand at least until the next blast of arctic air. **PJM operates the power grid that serves the 25 million people living between northern New Jersey and Washington D.C., with more than 71,600 MW of generating capacity on its system.** Source: [http://www.energycentral.com/sections/newsroom/nr\\_article.cf m?id=3601910](http://www.energycentral.com/sections/newsroom/nr_article.cf m?id=3601910)

## **Chemical Sector**

8. *January 29, CNN* — At least 8 missing after N. Carolina blast. A massive explosion blew apart a pharmaceutical supply plant Wednesday, injuring more than two dozen people — at least eight of them critically — and sending clouds of black smoke billowing into the sky. Authorities said people were killed in the blast, but they had no details on the number of fatalities. More than three hours after the blast, authorities said eight to 10 people were unaccounted for and believed trapped inside. The explosion at West Pharmaceutical Services, which makes syringes and other plastic medical supplies, occurred around 1:30 p.m. EST, when about 75 workers were on the job. The fire charred nearby woods and continued to burn hours after the explosion, gutting the massive complex. A makeshift triage center was set up on the lawn outside the factory, with medical helicopters and ambulances rushing the injured to medical facilities. Authorities evacuated an area about two miles in radius around the plant. **The blast, so powerful that it blew off house doors more than 1 1/2 miles away and sent debris flying as far away as 2 miles, stunned residents. "It was a tremendous explosion," City Manager Ralph Clark said.**

Source: <http://www.cnn.com/2003/US/South/01/29/nc.explosion/index.html>

9. *January 28, Bay City News Service* — **Accidents concern county officials.** California's Contra Costa County's refineries and chemical plants suffered 12 major accidents in a recent one-year period, causing officials to wonder why four years of strict safety laws have not improved this above-average number. **The finding came in the annual report of the Industrial Safety Ordinance, the county regulations enacted in 1999 that are widely viewed as the nation's toughest industrial safety regulations, according to county officials.** "Historically we've had an average of 10 major accidents per year," said Supervisor Donna Gerber as she reviewed the report at this morning's board meeting. "Does this mean we're getting better or that we're still in the place we've always been? Why doesn't that number go down?" Randy Sawyer, spokesman for the county's Hazardous Materials Program, told the board this morning that his group continues to review safety plans for the seven petrochemical facilities in Baypoint, Rodeo and Martinez that fall under county supervision. The Chevron Refinery and the General Chemical's sulfuric acid plant fall under near-identical regulations enacted by the city of Richmond. **Accidents included releases of more than 55,000 pounds of soot from the Equilon Martinez refinery in October of 2001 and plumes of gases that shot from General Chemical's sulfuric acid plant in Richmond a month later. Sulfuric gases were also released by Chevron's Richmond refinery and the Tesoro Golden Eagle Refinery near Martinez in the first two months of 2002.**

Source: <http://www.vallejonews.com/articles/index.cfm?artOID=27511webpage=79TD>>

10. *January 22, Reuters* — **Moody's issues report on global chemical industry. Moody's Investor Service anticipates fewer downgrades for the chemical industry in 2003. However, Moody's still expects trough-like conditions to continue throughout the year, leading to a moderately negative outlook. Moody's says the peak in the pricing cycle for most commodities in chemicals has now been pushed back to 2005. "Overall, we expect the chemical industry's financial performance to be similar to 2002," says Moody's Vice President/Senior Credit Officer John Rogers, who wrote the new Moody's Global Chemical**



Industry Outlook. He says the combination of elevated debt levels, high energy and natural gas prices, and the unusually long industrial downturn, will continue to cause some low B and Caa rated companies to default and some weaker Baa and Ba companies to be downgraded to the Ba and B rating categories. Rogers notes, however, that the outlook for industrial gas companies, a stable segment, remains positive. **The year 2002 weighed in as a tough one for the chemical industry as a whole, he says, with 25 companies and over \$36 billion downgraded versus only two upgrades.** Four companies became "fallen angels" during the year, their \$4.5 billion in debt moving into high-yield categories out of investment grade. **He also notes high natural gas prices, due to the cold winter and a potential war with Iraq, will have a negative impact on the industry in the first half of 2003.** Longer term a major credit risk he cites is a substantial increase in product liability lawsuits – notably for asbestos, lead paint, and other company-specific liabilities.

Source: [http://www.forbes.com/home\\_europe/newswire/2003/01/22/rtr855\\_085.html](http://www.forbes.com/home_europe/newswire/2003/01/22/rtr855_085.html)

[[Return to top](#)]

## **Defense Industrial Base Sector**

11. *January 29, Reuters* — **U.S. says 15,718 more reserve troops called up.** The U.S. military, preparing for possible war with Iraq, said on Wednesday it had activated almost 16,000 more Reserve troops, **swelling the total to almost 95,000, the biggest since the 1991 Gulf War.** Tens of thousands of part-time troops have been called to duty for the war on terror since the September 2001 attacks on the United States. Many are now moving to the Gulf region along with more than 100,000 U.S. regular troops, ships and warplanes in a new year's build-up for a possible war with Iraq. **The 15,718 Reserves newly called to active duty bring the total activated to 94,624. The weekly Pentagon announcement on Reserve and National Guard troops on active duty gave the following new totals: Army 64,741; Air Force 14,627; Marine Corps 8,729; Navy 5,476 and Coast Guard 1,051.** In addition, the United States recently ordered two more aircraft carriers to deploy to the Gulf, which will double to four the number of U.S. carriers — each with 75 warplanes — within striking distance of Iraq.

Source: <http://www.reuters.com/newsArticle.jhtml;jsessionid=4UVOUCXO0BYK4CRBAE0CFFA?type=topNews/a>>

[[Return to top](#)]

## **Banking and Finance Sector**

12. *January 29, Wall Street Journal* — **Antiterrorism law used to seize cash from Canadian fraud ring.** Federal agents, exercising civil-enforcement powers under the USA Patriot Act for the first time in a case unrelated to fighting terrorism, seized funds of a Canadian telemarketing ring that allegedly preyed on the elderly. **The Justice Department worked with Canadian authorities to shut down the scheme, which involved Canadian suspects based in Montreal targeting elderly Americans and funneling money to Jordanian and Israeli banks in Israel.** Mike Gunnison, head of the criminal unit for the U.S. attorney's office in New Hampshire, which brought the case, said recovering through asset forfeiture the \$4.5 million they found in foreign banks "would have been difficult, if not impossible," without using the

2001 Patriot Act. The government intends to use the money that is forfeited to pay restitution to the alleged victims of the fraudulent scheme. **The case could have implications for future prosecutions, since the Patriot Act will allow authorities to go after other funds that have been sent to offshore accounts, as long as those financial entities have U.S. branches. The act was designed to enhance law–enforcement officials' ability to root out terrorism, including tracking of financial sources, and to allow officials to conduct surveillance on suspects.**

Source: <http://online.wsj.com/article/0..SB1043793695314815664.00.ht ml>

13. *January 28, Comptroller of the Currency* — **Final Rule – anti–money– laundering requirements for foreign correspondent banks.** This bulletin transmits a final rule published by the U.S. Treasury Department on December 24, 2002, that amends the final rule published September 26, 2002. **The rule, effective immediately, extends the time from December 26, 2002, to March 31, 2003, for obtaining information from each foreign bank for which a covered financial institution maintains a correspondent account.** Information to be obtained includes the foreign bank's status as a "shell" bank, whether the foreign bank provides banking services to foreign shell banks, certain owners of the foreign bank, and the identity of a person in the United States to accept service of legal process. The September 26, 2002, final rule required that a covered financial institution obtain from a foreign bank a certification that contained the necessary information, or otherwise obtain documentation of the information. **With respect to correspondent accounts that existed on October 28, 2002, the final rule required the accounts be closed if the required information was not obtained by December 26, 2002. The December 24, 2002, final rule extends the deadline for obtaining the required information from December 26, 2002, to March 31, 2003.** Also attached to this bulletin is a correction to the September 26, 2002, final rule referenced above. The September 26 final rule contained an incorrect citation to a Web site maintained by the Federal Reserve Bank. The attached final rule correction, published January 6, 2003, contains the correct Web site address.

Source: <http://www.occ.treas.gov/ftp/bulletin/2003–3.doc>

[[Return to top](#)]

## **Transportation Sector**

14. *January 29, Reuters* — **Australia opens hi–tech passport checks. Australia launched the world's first automated passport checks using facial–recognition technology on Wednesday as it continued to tighten security at its borders in the aftermath of the September 11, 2001, attacks. At a cost of A\$1.2 million (\$708,000), the new SmartGate kiosk scans passport photos and compares them with the faces of travellers — replacing manual checks by customs officers at Sydney airport. The first phase of the project will apply only to crew members of national flag carrier Qantas Airways Ltd. It is likely to be expanded to staff of other international airlines, and other Australian airports, by 2004.**

Source: [http://asia.cnn.com/2003/TRAVEL/01/29/australia.security.air\\_ports.reut/](http://asia.cnn.com/2003/TRAVEL/01/29/australia.security.air_ports.reut/)

15. *January 29, Federal Register* — **Regulated navigation areas and security zones and escorted vessels in Philippine Sea, Guam, Apra Harbor, Guam and Tanapag Harbor, Saipan, Commonwealth of the Northern Mariana Islands. The Coast Guard is**

establishing regulated navigation areas (RNAs) and security zones for vessels determined to be in need of a Coast Guard escort by the Captain of the Port (COTP)Guam. The security zones for these escorted vessels will close all waters of Philippine Sea, Guam, Apra Harbor, Guam (including Cabras Island Channel), and Tanapag Harbor, Saipan, Commonwealth of the Northern Mariana Islands, within a 100-yard radius around an escorted vessel while in the RNA. **This action is necessary to protect personnel, vessels, and facilities from sabotage or other subversive acts, accidents, or other events of a similar nature. The RNAs will require vessels within 500 yards of an escorted vessel to travel at minimum safe speed and the security zones will prohibit unauthorized entry within a 100-yard radius of an escorted vessel in these RNAs.** This rule is not intended to replace or modify the existing RNAs and zones found in 33 CFR 165.1401, 33 CFR 165.1402, and 33 CFR 165.1404. **This rule is effective January 29, 2003.** Terrorist incidents within the United States on September 11, 2001 have called for the implementation of measures to protect U.S. seaports and transportation infrastructure. In addition, **national security and intelligence officials warn that future terrorist attacks against civilian targets are anticipated and that U.S. seaports are particularly vulnerable. These rules are intended to provide for the safety and security of the public, maritime commerce, and transportation by protecting persons, vessels, and seaport facilities in the waters of Philippine Sea, Guam, Apra Harbor, Guam, and Tanapag Harbor, Saipan, Commonwealth of the Northern Mariana Islands (CNMI).** These rules are intended to enable the COTP Guam to provide effective port security, while minimizing the publics' confusion and ease the administrative burden of implementing separate temporary security zones for each escorted vessel.

Source: <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-2061.htm>

16. *January 29, Associated Press* — **NTSB finds cable problem in crashed plane.** Federal investigators are trying to find out if shifting baggage contributed to the crash of a Beech 1900 turboprop plane in Charlotte, N.C. on Jan. 8. **Investigators said Tuesday they also found that control cables connected to the plane's tail weren't set at the proper tension level.** The cable problem could make a plane harder to fly because it would respond to the controls differently, aviation experts said. In a preliminary report, **the NTSB said turnbuckles that control tension on elevator control cables were set improperly, leaving one cable nearly 2 inches shorter than the other. If a cable is too slack, the pilot does not have full control of the elevator.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A58686-2003Jan 29.html>

17. *January 29, Washington Post* — **Passenger ignites seat on jet at Dulles.** A 64-year-old United Airlines passenger who had argued with the crew on his flight set his seat on fire at Dulles International Airport Tuesday night, officials said. The incident was one of two unusual events at Washington area airports within about 15 minutes, on an evening of increased overall security because of the president's State of the Union address. A small plane coming from Atlanta reported smoke in its lavatory as it approached Reagan National Airport, but the flight landed without incident. The Dulles passenger, who spoke Russian and little English, was belligerent at the gate before boarding Flight 383 for Chicago, said Transportation Security Administration spokesperson Heather Rosenker. Shortly after arriving at his seat, the man argued with a flight attendant. Tom Sullivan, a spokesman for the Metropolitan Washington Airports Authority, said the man then used a lighter to set his seat aflame. **A flight attendant**



extinguished the fire, and federal air marshals on the plane stood by the man as the aircraft turned around and headed back to the terminal about 6:30 p.m. The man was met by TSA officers, airport police and FBI agents at the terminal and was arrested and charged with disturbing a flight crew, a federal offense, Rosenker said.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A58174-2003Jan 28.html>

18. *January 29, Boston Globe* — **Box cutter found on jet at Logan.** A passenger of a United Airlines jet awaiting takeoff at Logan Airport Tuesday found a box cutter in the first-class cabin, prompting an evacuation of the plane and a federal investigation. Security officials said they saw no evidence that the box cutter was planted on the San Francisco-bound flight for a potential terrorist attack. But they said they have no idea how the box cutter – a large razor-like implement of the type thought to be used by hijackers from first-class cabins in the Sept. 11, 2001, terror attacks – got on the plane or who put it there. It was apparently the first discovery of a box cutter on an airliner since the federal government took over airport security last year. George Naccara, security director for the US Transportation Security Administration at Logan, said he believes the box cutter found Tuesday was on the jet, a Boeing 757, before it arrived in Boston from Denver International Airport at 1:46 p.m. Passenger Bob Ring, who sat in 2C, said a man in his row found the box cutter and turned it in to flight attendants, and the pilot grounded the flight. State Police quickly came on board with a bomb-sniffing dog, followed by plain-clothed officers.

Source: [http://www.boston.com/dailyglobe2/029/metro/Box\\_cutter\\_found\\_on\\_jet\\_at\\_Logan+.shtml](http://www.boston.com/dailyglobe2/029/metro/Box_cutter_found_on_jet_at_Logan+.shtml)

19. *January 28, Austin Business Journal* — **28 ABIA workers charged with falsifying clearance applications.** Twenty-eight employees at Austin-Bergstrom International Airport in Texas have been accused of using false information to obtain access badges for secure areas at ABIA. Federal authorities arrested 15 of the defendants Tuesday as part of Operation Tarmac, designed to promote heightened security at U.S. airports. The defendants made initial appearances Tuesday in U.S. District Court in Austin. Arrest warrants have been issued for the remaining suspects, according to the U.S. Attorney's Office. The case stems from an investigation that began in October. During the course of the investigation, **28 employees were discovered to have repeatedly lied to obtain security clearances. All had active security badges when they were charged.** On Jan. 21, a federal grand jury handed up the sealed indictments. The defendants are charged with obtaining access badges by providing false information on security clearance forms. **The badges permit access to all restricted and secure areas at ABIA, including the control tower and the interior and cargo holds of airplanes.**

Source: <http://austin.bizjournals.com/austin/stories/2003/01/27/daily27.html>

20. *January 28, CommsDesign* — **FAA technologist urges better security in network boxes.** In a keynote address at the Comnet 2003 conference Tuesday, the chief information officer of the U.S. Federal Aviation Administration (FAA) urged networking equipment designers to add security capabilities to their systems earlier in the design process. To aid the effort, the FAA is working with manufacturers to define security requirements for the FAA's networks, said Daniel Mehan, assistant administrator for information services and CIO of the federal agency. "We're trying to reach a meeting of the minds so that we can get more security features into initial designs," he said. Mehan's request to industry is just one point in the FAA's

three-layer approach to bringing higher levels of security to its network, which manages an average of 350,000 flights and two-million passengers per day. While the progression of hacker knowledge has decreased, the strength of their attacks has gotten stronger, Mehan said. "This is an area where you always have to be prepared," he said. The first layer of the FAA's approach involves personnel security, and is intended to educate and automate the security of FAA personnel. The second involves physical security; the final layer focuses on cybersecurity. To improve cybersecurity, Mehan said the FAA and all business must harden individual network and system elements, isolate elements to avoid viral attacks, and backup elements to support event recovery. **Having networking equipment developers add security to their designs is one element of cybersecurity, but Mehan also called for the isolation of mission-critical components. The FAA isolates the network-attached storage systems that house vital flight information, for example.**

Source: <http://www.commsdesign.com/news/OEG20030128S0031>

21. *January 28, Government Executive Magazine* — **Transportation IG outlines department management challenges.** Facilitating the transfer of two agencies to the Homeland Security Department, cutting costs at the Federal Aviation Administration and complying with the president's management agenda top the challenges facing the Transportation Department in 2003, according to the department's Inspector General. In a report released Jan. 23, **Transportation Inspector General Kenneth Mead detailed the major issues facing the department, including shifting the Coast Guard and Transportation Security Administration over to the newly created Homeland Security Department.** According to Mead, the shift of those two agencies gives Transportation Department officials the opportunity to focus on the core missions of transportation safety and mobility. But the department would still play an important role in transportation security, the IG's report said. **But until TSA joins the new department, agency officials should focus on training the new baggage screener workforce and controlling costs, the IG recommended.** The agency had \$8.5 billion in contracts at the end of 2002. The Transportation Department has an annual IT budget around \$2.5 billion and invests 2 percent to 3 percent of its IT budget in computer security, according to the IG. **To better align itself with the president's management agenda, the department needs to strengthen computer security and information technology investment controls.** "This must be done with a view toward cost-effective system acquisitions and reducing system vulnerabilities to cyberattacks," said the report. The full text of the report is available at [http://www.oig.dot.gov/show\\_pdf.php?id=977](http://www.oig.dot.gov/show_pdf.php?id=977) .  
Source: <http://www.govexec.com/dailyfed/0103/012803t1.htm>

[[Return to top](#)]

## **Postal and Shipping Sector**

22. *January 28, U.S. Customs Service* — **Container Security Initiative expands beyond the megaports.** U.S. Customs Commissioner Robert C. Bonner and Kjell Jansson, Director General of the Swedish Customs Service, announced on Tuesday that **the government of Sweden has agreed to participate in the U.S. Customs Container Security Initiative (CSI).** CSI is a U.S. Customs initiative designed to prevent the smuggling of terrorist weapons in ocean-going cargo containers. **Under terms of the declaration announced Tuesday, U.S. Customs officers will be stationed at the port of Göteborg (Gothenburg), the first**

**European port outside the top 20 mega ports to join CSI.** "Today, we have begun the expansion of CSI beyond the top 20 megaports by entering into a CSI agreement that will make the port of Göteborg a CSI port. This is the first expansion of CSI beyond the top 20 ports in Europe. Now that we have implemented CSI at most of the top 20 ports, we are quickly expanding CSI to all ports that ship substantial amounts of cargo to the United States, and that have the infrastructure and technology in place to participate in the program," said Commissioner Bonner.

Source: [http://www.customs.gov/xp/cgov/newsroom/press\\_releases/01282\\_003.xml](http://www.customs.gov/xp/cgov/newsroom/press_releases/01282_003.xml)

[[Return to top](#)]

## **Agriculture Sector**

23. *January 28, Ag Web* — **EU to resume most U.S. poultry imports. The European Union (EU) has agreed to resume imports of U.S. poultry except from Arizona, California, and Nevada.** The EU had banned all imports of U.S. poultry when Exotic Newcastle Disease was discovered in California. The authorization to resume trade will become effective upon publication in the EU's Official Journal either Wednesday or Thursday.

Source: [http://www.agweb.com/news\\_show\\_news\\_article.asp?file=AgNewsArticle\\_20031281353\\_1936newscat=GN](http://www.agweb.com/news_show_news_article.asp?file=AgNewsArticle_20031281353_1936newscat=GN)

24. *January 28, IcNewcastle* — **Britain is just as vulnerable to FMD as it ever was.** Future foot-and-mouth disease (FMD) outbreaks in the UK could spread as quickly and easily as the 2001 epidemic under present sheep farming methods, North-East academics warned today. **A report by Newcastle University and The Institute of Logistics and Transport says gaps in records of the animals and the number of their movements are leaving the country vulnerable to another such devastating outbreak.** The rapid and extensive spread of the 2001 outbreak was exacerbated by sheep movements, with animals from Northumberland which were harbouring the disease being moved from Hexham to Devon, via a Cumbrian auction mart. Academics at the university's Centre for Rural Economy say the problem still exists and warned that some animal movements were not being recorded, making traceability even harder. **To tackle the problem, they are calling for every sheep to have its individual tag or passport, like cattle, and auction marts and abattoirs to be located closer to the regions where sheep are reared, so live animal journeys are kept to a minimum. The report, which followed a year long study, also recommended a strategic review of the fat lamb supply chain.**

Source: <http://icnewcastle.icnetwork.co.uk/0100news/0100local/page.cfm?objectid=12577760id=50081>

[[Return to top](#)]

## **Food Sector**

25. *January 29, New York Times* — **The question of irradiated beef in lunchrooms. The farm bill that was passed last May directs the Agriculture Department to buy irradiated beef for the federal school lunch program. It will be up to local school districts to decide if they**

**want it.** Americans have been reluctant to buy food that is irradiated, a process that uses electrons or gamma rays to kill harmful bacteria like salmonella and E. coli 0157:H7, which cause food poisoning. Some people fear, wrongly, that the food is radioactive. Others are concerned that the process hasn't been tested well. Because the word irradiation conjures up radioactivity and, more recently, the method by which anthrax spores have been killed, the industry has tried to keep it off food packaging. It is lobbying to use a word with which people are more comfortable: pasteurized. A farm bill provision, added by Senator Tom Harkin, the Iowa Democrat, directs the Food and Drug Administration to look for a less fear-inducing word. Senator Harkin, a longtime proponent of food safety, is also responsible for the language in the bill that directs the Agriculture Department to buy irradiated meat. **Although the Agriculture Department is authorized to offer irradiated meat to schools, the secretary of agriculture, Ann M. Veneman, is moving slowly. So far, it is served only in schools in a pilot program in Minneapolis. According to the Center for Food Safety, a nonprofit Washington advocacy group, which opposes irradiation of food, of more than 1,500 comments the Agriculture Department received from the public on the subject, two-thirds were against it.**

Source: <http://www.nytimes.com/2003/01/29/dining/29WELL.html>

26. *January 28, United Press International* — **Foodborne illnesses increasing. A rising number of outbreaks of foodborne illnesses contracted from eating fresh fruits and vegetables point to the need for better food handling practices from grower to consumer, scientists and federal health experts said Tuesday.** "Our data suggest that foodborne outbreaks associated with fresh produce consumption have increased over the last three decades," said Dawn Norton, an Epidemic Intelligence Service officer in the U.S. Centers for Disease Control and Prevention's foodborne and diarrheal diseases branch. Norton noted up to 3 percent of foodborne outbreaks could be attributed to contaminated fruit and vegetables. "The actual proportion may be slightly higher," she said, because the figures do not include salads. Three plant and food scientists noted in a recent study that Salmonella, E. coli and other pathogens have been detected on seeds, sprouts, unpasteurized fruit juice, raw fruits and vegetables. Produce-related outbreaks of pathogens normally associated with meat have been on the increase for the past 20 years, J.W. Buck, an author of the study and a plant pathologist at the University of Georgia, told United Press International. "This trend is likely attributable to an increased consumption of fresh produce by Americans, and thus increased exposure to pathogens that may be present," Norton said. **A 1999 study by the Food and Drug Administration (FDA) found about 4 percent of imported produce was contaminated with either Salmonella or another bacteria, Shigella. A FDA study of domestic produce in 2000 found 12 samples out of 919 tested positive for the presence of Salmonella, Shigella and E. coli.**

Source: <http://www.upi.com/view.cfm?StoryID=20030128-021244-3377r>

[\[Return to top\]](#)

## **Water Sector**

27. *January 29, Atlanta Journal Constitution* — **Tri-state water talks stall.** The settlement agreement signed earlier this month to give metro Atlanta more drinking water continues to threaten the fragile tri-state water negotiations. **Alabama this week ended a decade-old truce**

with Georgia, renewing its legal attack to stop the U.S. Army Corps of Engineers from giving metro Atlanta more water from Lake Lanier and the Chattahoochee River. Florida immediately denounced the deal made between Georgia, the corps, and other parties. A Florida spokesman on Tuesday said officials there were also considering legal action. Both Alabama and Florida have said they want to continue the tri-state water-sharing talks after Atlanta's water deal is dissolved. If the states cannot come to an agreement by the July 31 deadline, or cannot agree to extend the deadline, the matter will go to the U.S. Supreme Court. On Monday night, Alabama Gov. Bob Riley announced his state had filed a motion in U.S. District Court for the Northern District of Alabama to stop the settlement agreement, which would give metro Atlanta counties as much as 50 percent more water than they got last year for at least the next 10 years. A 1990 lawsuit filed by Alabama against the corps was intended to stop the corps from doing exactly that: Giving metro Atlanta more water for homes and businesses. Georgia joined that lawsuit on the side of the corps; Florida sided with Alabama. The three states called a truce in 1992, eventually leading to the tri-state water negotiations, which began in 1998.

Source: <http://www.accessatlanta.com/ajc/metro/0103/29water.html>

28. *January 29, Indianapolis Star* — **Better wastewater treatment, changes in safety standards could cost Indiana up to \$13.9 billion.** Improving wastewater treatment and ensuring safe drinking water throughout Indiana could cost billions of dollars more than previously believed, according to a study released Monday. **The study conducted by researchers at the Center for Urban Policy and the Environment at Indiana University and Purdue University Indianapolis (IUPUI) estimates it would take \$12.4 billion to \$13.9 billion during the next 20 years to correct sewer overflow problems, meet federal drinking water standards, and stem pollution from stormwater and failing septic systems in communities large and small.** That is 35 percent to 53 percent higher than the U.S. Environmental Protection Agency's previous estimate of \$9.1 billion, study author Greg Lindsey, director of the IUPUI center, told the state Senate Environmental Affairs Committee. He said the EPA estimates did not include septic systems and stormwater controls.

Source: <http://www.indystar.com/print/articles/9/018642-6579-009.htm>

[[Return to top](#)]

## **Public Health Sector**

29. *January 29, Boston Globe* — **State adds 17 diseases to reportable list. Reflecting concerns about bioterrorism as well as the emergence of new diseases on U.S. shores, the state Department of Public Health yesterday announced that Massachusetts doctors must report all cases of 17 diseases, including smallpox, plague, Norwalk virus, and the flu.** When the rule goes into effect in about two weeks, it will expand the state's roster of reportable diseases to 78. **Once a disease is reported, its spread can be tracked by public health officials, who can then move to contain the disease.** The new list includes flesh-eating bacteria and Q fever, a bacterial condition that humans catch from the waste of barnyard animals. Some of the diseases on the list, such as smallpox, have not been seen in Massachusetts in many years. **"Most of the diseases we're adding are extremely rare," said Gillian A. Haney, surveillance program manager in the state's Bureau of Communicable Disease Control. "But we wanted the list to reflect the reality of new threats."** Department



of Public Health executives concede that the new regulation will add to the mountain of paperwork already confronting physicians. "We acknowledge the burden on the providers, and we are working with them to streamline the process the best we can," said Robert S. Goldstein, director of the agency's division of epidemiology and immunization.

Source: [http://www.globe.com/dailyglobe2/029/metro/State\\_adds\\_17\\_diseases\\_to\\_reportable\\_list+.shtml](http://www.globe.com/dailyglobe2/029/metro/State_adds_17_diseases_to_reportable_list+.shtml)

30. *January 29, American Forces Press Services* — **Researchers test enzyme as anthrax treatment. An anthrax-killing enzyme now being tested by the U.S. Defense Department may one day be used as a medical treatment against the deadly bacteria, a researcher said.** The enzyme, lysin, "is like a smart bomb that kills anthrax, but doesn't kill anything else," noted Dr. John Carney, a pharmacologist with the Defense Advanced Research Projects Agency (DARPA). "This could be an unique treatment against anthrax that wouldn't cause side effects." Carney has worked three years with DARPA-contracted research microbiologists at Rockefeller University in New York, in developing more effective medical therapy for anthrax. **Lysin attacks anthrax by dissolving a hole in the bacteria from the inside out, Carney explained. Water surrounding the ruptured anthrax cell rushes in, he continued, causing it to burst.** Persons can receive vaccinations for protection against anthrax, Carney pointed out, while Cipro, doxycycline, penicillin and other antibiotics are used as treatment for unvaccinated people who've been, or may have been, exposed to the bacteria. Yet, some persons might be allergic to the antibiotics used to battle anthrax, he acknowledged. In addition, he said, broad-spectrum antibiotics are indiscriminate. They kill all bacteria, even beneficial ones, and that can cause side effects such as diarrhea. **He said the new enzyme, on the other hand, has the potential for fewer side effects because it would kill only anthrax bacteria.**

Source: [http://www.defenselink.mil/news/Jan2003/n01292003\\_200301293.html](http://www.defenselink.mil/news/Jan2003/n01292003_200301293.html)

[\[Return to top\]](#)

## **Government Sector**

31. *January 29, Washington Post* — **Terrorism agency planned; center to integrate intelligence, analysis.** President Bush announced plans Tuesday night for a new center to integrate intelligence on terrorism collected at home and abroad, saying it was necessary to create the most comprehensive picture of possible threats to the United States and its citizens. **A senior administration official said the new Terrorist Threat Integration Center will assess intelligence gathered by the CIA, Justice Department, Pentagon and Department of Homeland Security and provide "seamless" analysis of the information to the president and other senior policymakers. The new center is expected to take over compilation of the integrated threat matrix -- a day-by-day accounting of potential threats -- given to President Bush and other senior national security officials each morning.** The new center is aimed at helping to eliminate remaining barriers between the nation's intelligence agencies, particularly the CIA and FBI, over sharing and analyzing intelligence. **The center will be placed directly under the supervision of Director of Central Intelligence George J. Tenet, reinforcing Tenet's role as Bush's senior intelligence adviser, officials said.** The threat integration center will analyze intelligence and ensure the information is shared throughout the federal government as well as with state and local authorities. It also will have the authority to set requirements for all intelligence agencies and assign collection operations to the CIA, the

Pentagon, the FBI and, through Homeland Security, to state and local law enforcement authorities. **Bush has told aides he wants the center to be created "right away," the official said. An interagency task force is being formed to work out the details. One idea is to take the CIA's counterterrorism center, now manned by more than 1,000 people and the oldest of the nation's integrated intelligence centers, and move it to a new facility outside CIA headquarters in Langley, according to one senior official. The new threat center, with senior terrorism analysts from the CIA, FBI, Pentagon, Homeland Security Department and other agencies, would be on one floor of the new facility. The CIA counterterrorism center would be located on other floors.** In another move to strengthen analysis of potential threats, the officials said, the FBI has given the collection and dissemination of intelligence the same priority that it has in the past applied to the collection of evidence for prosecution of crimes. A new FBI executive assistant director will be named and given authority to direct intelligence units to be established at all FBI field offices.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A58384-2003Jan 29.html>

**32. *January 29, New York Times* — Bush enlarges case for war by linking Iraq with terrorists.**

President Bush said Tuesday night that there was intelligence showing that Iraq was helping and protecting terrorists. He warned that Saddam Hussein could distribute weapons of mass destruction to terrorists who could use them against the United States. Administration officials have long been suspicious that there are hidden links between Saddam Hussein and terrorist groups, relations Iraq could exploit to attack the United States while masking its responsibility. **"Evidence from intelligence sources, secret communications, and statements by people now in custody, reveal that Saddam Hussein aids and protects terrorists, including members of Al Qaeda," the president said in his speech.** Just a few months ago, the C.I.A. told Congress that Iraq was striving to develop weapons of mass destruction but was unlikely to orchestrate terrorist attacks in the United States unless Washington struck Iraq first. The C.I.A. has never amended that public assessment. **"Baghdad for now appears to be drawing a line short of conducting terrorist attacks with conventional or C.B.W. against the United States," the C.I.A. said, referring to chemical and biological weapons, in an Oct. 7 letter to Congress. "Should Saddam conclude that a U.S.-led attack could no longer be deterred, he probably would become much less constrained in adopting terrorist actions," the C.I.A. added. "Saddam might decide that the extreme step of assisting Islamist terrorists in conducting a W.M.D. attack against the United States would be his last chance to exact vengeance by taking a large number of victims with him."**

Source: <http://www.nytimes.com/2003/01/29/politics/29MILI.html>

**33. *January 29, New York Times* — U.S. deficit could top \$300 billion.** White House officials suggested today that the federal budget deficit could surpass \$300 billion this year, setting a record. **Mitchell E. Daniels Jr., director of the White House Office of Management and Budget, told the Reuters news service that the deficit could hit 3 percent of gross domestic product, which would put the deficit above \$300 billion.** That is slightly higher than what Mr. Daniels and other administration officials have been hinting in recent weeks, but many outside economists say the actual deficits could turn out to be even higher, especially if the United States goes to war with Iraq. **The Congressional Budget Office, the nonpartisan agency that makes its own estimates of fiscal trends, is expected to report on Wednesday that the deficit for 2003 will be at least \$175 billion — but that is without any allowance for Mr. Bush's \$674 billion, 10-year tax plan or the costs of a possible war.**

Source: <http://www.nytimes.com/2003/01/29/business/29BUDG.html>

34. *January 29, Washington Times* — **More countries issue ID cards to illegal aliens in U.S.** Guatemala, Honduras, Poland, Peru and El Salvador, aware of Mexico's success in getting identification cards to its citizens in the United States, including those here illegally, have begun or are considering issuing cards of their own, federal officials said yesterday. Known as "**matricula consular cards**," the digitally-coded documents are being used by Mexican nationals in the United States as legal forms of identification. The laminated cards, which do not list the holder's immigration status, also are being used as identification by those stopped or questioned by police. Nearly a million of the cards were issued last year by the Mexican government to Mexican nationals now in this country. **In the wake of the Mexican program, Guatemala began issuing similar identity cards last year known as the "Tarjeta de Identificacion Consular."** It plans eventually to make them available to the estimated 327,000 Guatemalans living in the United States. Honduras, Poland and Peru have the matter under serious consideration. El Salvador has begun issuing a secure, in-country identification card known as the Documento Unico de Identidad (DUI), but has not said **whether it will expand the program.** Hundreds of state and local governments, along with 798 police agencies and 74 banks, now accept the cards for identification purposes — despite warnings by federal law-enforcement authorities of potential widespread fraud involving the cards. **Last week, the General Services Administration suspended recognition of the cards at federal facilities pending an investigation. The GSA said once the probe is completed, a recommendation would be made to federal law enforcement and security agencies to ensure the cards' integrity and security.**

Source: <http://www.washingtontimes.com/national/20030129-94046601.htm>

[[Return to top](#)]

## Emergency Services Sector

35. *January 29, Washington Post* — **Fairfax to confine students in case of terrorist attack.** If the Washington area were hit by a chemical or biological attack, Fairfax County students would be kept in locked-down schools, inaccessible to parents, while teachers helped undress and shower any who needed decontamination, according to a plan adopted by school authorities. **While the county is the first in the Washington region to develop school procedures for dealing with chemical attacks, the U.S. Department of Education plans to recommend this spring that school systems across the nation do likewise, federal officials said.** After the terrorist attacks of Sept. 11, 2001, "that's what it has come to," said James McLain, security coordinator for Fairfax schools. "We have the federal government telling us that terrorist attacks are not a matter of if, but of when." **Fairfax's security plan is of a type known as "Shelter in Place," and it is predicated on the notion that in a chemical attack, people are often safest if they remain inside. Such plans have been put in place by some school districts and local governments near nuclear plants, armories and chemical factories.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A57229-2003Jan 28.html>

36. *January 29, USA Today* — **Troop call-ups leave shortages at home.** The Pentagon's call-up of 144,000 National Guard and Reserve troops is straining many law enforcement agencies, from small-town police departments to state highway patrols and federal bureaus. **The number**

of "weekend warriors" called to full-time duty since the Sept. 11 terrorist attacks is the largest since the Gulf War a decade ago. More are expected to be shipped overseas in preparation for a possible war against Iraq. And some law enforcement officials worry they could be short-handed on the homefront. In Monroe, Ga., population 11,407, Police Chief Keith Glass is an officer in the Army Reserve. Six of his 36 police officers serve part time in the National Guard or Reserves. The Spokane, Wash., police department has 19 of its 300 officers in Reserve or Guard units. Three have been called up for a one-year stint. Though that might seem a small number, it taxes the department. "If somebody calls in sick, it's a problem," spokesman Dick Cottam says. "Losing somebody for a year hurts." In West Virginia, the 565 state troopers include 51 Guard and Reserve members. Among them is the superintendent, Howard Hill. A few of the troopers already have been called to duty, causing some delays in response time by the state police. "The effects of a (full) call-up would be devastating," Hill says. The Texas state Department of Criminal Justice has lost more than 400 corrections officers to Guard and Reserve call-ups during parts of the past 18 months, according to spokesman Larry Todd. The department has drafted a contingency plan that includes more prison lockdowns and less inmate movement to deal with the shortage of prison guards. **Though concern is directed at law enforcement, the call-ups also have affected firefighters, nurses, doctors and the aviation industry.**

Source: [http://www.usatoday.com/news/nation/2003-01-28-troops-shortage-usat\\_x.htm](http://www.usatoday.com/news/nation/2003-01-28-troops-shortage-usat_x.htm)

37. *January 29, New York Times* — **Accident underscores lack of cellphone tracking.** City, state and federal elected officials said on Tuesday that the disappearance of four teenagers in a Bronx boating accident has underscored an intolerable delay in creating a tracking system to trace the location of emergency calls from cellphones in New York. **One of the teenagers placed a 12-second 911 call from his cellphone on Friday night as their boat sank in the icy waters off City Island. Police officials have said the operator mishandled the call by not relaying it to emergency units. But they have also said that the rescue crews were likely too far away to have arrived in time and that the call was too short and faint to pinpoint the boat's location.** United States Senator Charles E. Schumer was one of several officials who said that long-promised improvements to enable the 911 system to track cellphone calls might have provided critical information in quickly locating the boat. But whereas Schumer criticized state officials for the delays, other officials pointed fingers at federal regulators or the city. **Such sophisticated tracking systems are still rare around the country, experts said, but Houston and Rhode Island have the ability to trace cellphone calls to a specific longitude and latitude. New York City is about three years away from installing such a system, said Michael J. Farrell, the New York Police Department's deputy commissioner for strategic initiatives.**

Source: <http://www.nytimes.com/2003/01/29/nyregion/29CALL.html>

[\[Return to top\]](#)

## **Information and Telecommunications Sector**

38. *January 30, Post Newsweek Tech Media* — **Budget strain won't stop state and local IT funding, report says. Despite facing billions of dollars in budget deficits, states will find the funds necessary for mission-critical technology projects in 2003,** according to the market research firm of Input Inc., Chantilly, Virginia. According to Meredith Luttner, Input's

manager of state and local market development services, "**Homeland security drives most of the mission—critical projects that will be moving forward this year. States cannot afford to put programs that are critical to constituent safety, such as public safety communications systems and health networks, on hold.**" The findings are based on a report Input conducted of the top 2003 program priorities in Virginia, New Jersey and California. The report reviews 2003 priorities in the three states and highlights specific projects slated for procurement this year. Of the states covered in the report, **California and New Jersey are moving forward with projects to construct and implement enhanced 911 networks and automated child enforcement systems, while California and Virginia are undertaking projects to enhance information security.** The study acknowledges that program priorities and the depth of the budget problem vary from state to state. According to the National Association of State Budget Officers, the aggregate budget shortfall among the states is about \$50 billion.

Source: [http://www.GovernmentComputerNews.com/vol1\\_no1/daily-updates/21010-1.html](http://www.GovernmentComputerNews.com/vol1_no1/daily-updates/21010-1.html)

39. *January 28, Associated Press* — **Hunt for source of Internet attack tough, experts say.**

Exhaustive reviews of the blueprints for the attacking software for last weekend's attack on the Internet are yielding few clues to its origin or the author's identity. Many top experts believe the programming for the Internet worm was based on software code published on the Web months ago by a respected British computer researcher, David Litchfield, and later modified by a virus author known within the Chinese hacker community as "Lion." That **altered computer code was published in the online hangout for the Hacker Union of China, known as Honker,** a group active in skirmishes between American and Chinese hackers that erupted in 2001 after the forced landing of a U.S. spy plane. But **experts said it was impossible to say whether members of that Chinese hackers organization unleashed the damaging worm.** Unlike attacking software used in some previous high-profile Internet disruptions, **the latest code is exceedingly condensed and doesn't include references to hacker aliases or locations. It also used a transmission method that made it especially easy for its author to throw off investigators by falsifying his digital trail.** Experts said they found no distinctive programming techniques that the new worm's author employed that might help identify him. Investigators were comparing its blueprints to libraries of other malicious software. Miles McNamee, a top official with the U.S. technology industry's Internet early warning center, said this week the damage from the attack could approach several billion dollars. Others said the FBI was confident Tuesday that the infection started in Korea and Japan. That doesn't mean its author lived there, but that the first vulnerable computers were there. All this doesn't mean investigators won't get lucky: **Hackers routinely draw the FBI's attention by claiming credit for their online exploits in chat rooms.**

Source: <http://www.siliconvalley.com/mld/siliconvalley/news/5053136.htm>

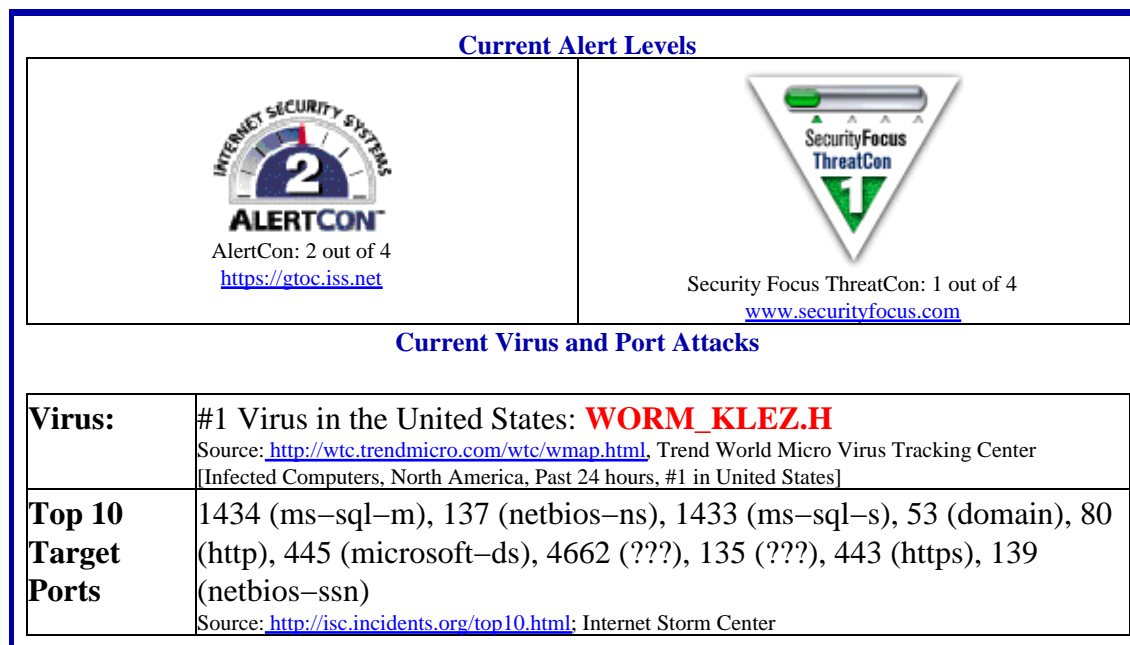
40. *January 28, Government Computer News* — **Better patch management could have slowed Slammer.** The failure of many organizations to apply a patch that had been available since the summer contributed to the spread of the worm known as "SQL Slammer" over the weekend. An estimated 250,000 servers were infected. According to John Schwarz, president of Internet security technology company Symantec Corporation, **the failure to prevent its spread is a reflection of the complex nature of network security and the lack of resources devoted to it. The technology to secure systems is in place; the problem is in managing information.** Speaking at a trade show in Washington today, he said: "Many people have implemented the right techniques and tools to defend themselves," but "we have pretty much failed" at policy



enforcement for security. Patch management is a critical element in security. **The problem often is not ignorance of the vulnerability or of the fix. The cost in time and resources of deploying security patches for large enterprises can be prohibitive. Many organizations assign patching a low priority until the threat materializes as a real attack,** he said.

Source: [http://www.gcn.com/vol1\\_no1/daily-updates/21016-1.html](http://www.gcn.com/vol1_no1/daily-updates/21016-1.html)

### Internet Alert Dashboard



[[Return to top](#)]

## General Sector

41. *January 29, Associated Press* — **Germany tightens security at U.S. embassy.** Police tightened security Wednesday at U.S. and Israeli embassies in the German capital, acting on intelligence reports suggesting an attack was planned. **Foreign security services passed on "general information about a concrete attack" on the embassies, police spokesman Hansjoerg Draeger said. He refused to give further details.** German officials have repeatedly warned terrorists could strike here, with U.S. and Israeli interests considered likely targets. Security in the capital is also tight around the British Embassy.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A60180-2003Jan 29.html>

42. *January 29, Associated Press* — **Pakistani police arrest 21 suspected Islamic militants.** Police raided an office of an Islamic militant group in a town in remote western Pakistan, seizing weapons and detaining 21 suspects, authorities said Wednesday. Most of the men are believed to be members of Jamiat-ul-Ansar, a group previously known as Harkat-ul-Mujahadeen, police said. They were arrested Tuesday on a raid on an office in Dera Ismail Khan, 180 miles southwest of the capital, Islamabad. The suspects are believed to have gone underground to avoid arrest when Pakistan banned Harkat-ul-Mujahadeen and four other radical groups after a Dec. 13, 2001 attack on the Indian parliament, for which New Delhi

blamed Pakistan-based militants. **The group is one of the main factions fighting in Indian Kashmir for its merger with Pakistan. Members also fought alongside the Taliban in Afghanistan against U.S.-led coalition forces that overthrew the hardline Islamic militia. Police have accused members of an offshoot of the group of targeting McDonald's and Kentucky Fried Chicken outlets in Pakistan. Members of another Harkat-ul-Mujahadeen splinter group are on trial for allegedly masterminding the June 14 car bomb attack outside the U.S. Consulate that killed 12 Pakistanis and injured 50 others.**

Source: [http://www.usatoday.com/news/world/2003-01-29-pakistan-militants\\_x.htm](http://www.usatoday.com/news/world/2003-01-29-pakistan-militants_x.htm)

43. *January 29, Associated Press* — **British police arrest four terror suspects.** Police arrested four terror suspects in separate raids early Wednesday in northern England's Greater Manchester area. **The four men, all in their 30s, were detained under the Terrorism Act 2000 and are to be taken to London for questioning by anti-terrorist police.** Three of the men were arrested at separate addresses in Manchester, and the fourth man in Bury, north of the city, police said. **The raids were unrelated to the murder of Detective Constable Stephen Oake, who was fatally stabbed during an anti-terrorist raid in Manchester earlier this month, police said.**

Source: [http://www.usatoday.com/news/world/2003-01-29-britain-arrests\\_x.htm](http://www.usatoday.com/news/world/2003-01-29-britain-arrests_x.htm)

44. *January 29, New York Times* — **Europeans warn of terror attacks in event of war in Iraq.** European investigators have evidence that over the past six months, Islamic militants have been recruiting hundreds of fellow Muslims to carry out attacks in the event of a war against Iraq, according to French and other European antiterrorism experts. **A French expert, who requested anonymity, said one threat to Europe came from radical groups who have links with Chechnya and have learned how to make chemical weapons, either at training camps in Afghanistan or while serving in the Soviet Army. He said Chechnya was now a kind of "neo-Afghanistan," a new training ground and staging area for anti-Western terrorists. What was just a working thesis a few months ago, he said, has been validated by new information about intense recruiting, training and a focus on chemical weapons. In both Spain and Britain, the police reported finding chemical protection suits during raids last week in Barcelona and London.** In France, the police prevented "serious attacks" in Paris in December, probably including attacks using chemical weapons, the French expert said. Western Europe is home to about 15 million Muslim immigrants and while a vast majority are peaceful citizens opposed to terrorism, their presence provides a recruiting ground and a cover for sleeper cells. **Investigators said links between bases in Chechnya and cells in Europe had been known for some time. In recent days, some of the links have been publicized.** Fears of terrorist actions against European cities in case of war against Iraq are a concern throughout Western Europe, diplomats said. **On Monday, the Italian interior minister, Giuseppe Pisanu, told Parliament in Rome that terrorism is a major and growing threat in Italy, and added, "The internal and international terrorist threat would be even more worrying if there were a war in Iraq."** The Italian police last week arrested five Moroccans found near Venice with plastic explosives and a detailed map of London. **In France, the antiterrorism expert said terrorist attacks in European capitals would be "a price we may have to pay" if war breaks out.** "We have evidence of a great deal of recruitment" by radical Islamic groups that would seek to take advantage of a war situation to sow mayhem, he said.

Source: <http://www.nytimes.com/2003/01/29/international/europe/29FRA N.html>

## **NIPC Products & Contact Information**

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following NIPC products:

[NIPC Advisories](#) – Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

[NIPC Alerts](#) – Alerts address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

[NIPC Information Bulletins](#) – Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

[NIPC CyberNotes](#) – CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

### **NIPC Daily Open Source Report Contact Information**

Content and Suggestions:	Melissa Conaty (202-324-0354 or <a href="mailto:mconaty@fbi.gov">mconaty@fbi.gov</a> ) Kerry J. Butterfield (202-324-1131 or <a href="mailto:kbutterf@mitre.org">kbutterf@mitre.org</a> )
Distribution Information	NIPC Watch and Warning Unit (202-323-3204 or <a href="mailto:nipc.watch@fbi.gov">nipc.watch@fbi.gov</a> )

### **NIPC Disclaimer**

The NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal NIPC tool intended to serve the informational needs of NIPC personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The NIPC provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.